

EXHIBIT 6

(June 17, 2021, Warrants)

Executed June 21, 2021

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 3:07 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
487 E PETAL DEW AVENUE,
LAS VEGAS, NEVADA 89183

Case No. 2:21-mj-514-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-1.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Daniel J. Albregts
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: June 17, 2021 2:34 p.m.

City and state: Las Vegas, Nevada



Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge

Printed name and title

US-001007



SEALED

ATTACHMENT "A-1"

PREMISES TO BE SEARCHED – SUBJECT PREMISES 1

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

487 Petal Dew Avenue, Las Vegas, Nevada 89183 is a residential home leased by Paul ENGSTROM. Subject Premises is a two story, single family residence having primarily yellow beige stucco exterior with beige trim. The residence has a single car garage door that is beige in color and faces north. The numbers "487" are affixed to the east side of the residence above the garage. The front door of the residence is an unknown color encased by a white security door. Photo of Residence:



ATTACHMENT "B"**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
- 2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
- 4 control the device, such as viruses, Trojan horses, and other forms of
- 5 malicious software, as well as evidence of the presence or absence of security
- 6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
- 9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
- 12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
- 14 well as documentation and manuals, that may be necessary to access the
- 15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
- 17 device;
- 18 ix. records of or information about the device's Internet activity, including
- 19 firewall logs, caches, browser history and cookies, "bookmarked" or
- 20 "favorite" web pages, search terms that the user entered into any Internet
- 21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

- 4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;
- 9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.
- 13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.
- 17
18
19
20
21
22
23
24

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 3:08 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 304 E. SILVERADO RANCH BOULEVARD,
 UNIT 1110
 LAS VEGAS, NEVADA 89183

Case No. 2:21-mj-515-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-2.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 *(not to exceed 14 days)*☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Daniel J. Albregts
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.Date and time issued: June 17, 2021 2:34 p.m.City and state: Las Vegas, Nevada

A handwritten signature in blue ink, appearing to read "Daniel J. Albregts".

Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
Printed name and title

Inventory of the property taken and name(s) of any person(s) seized:



SEALED

ATTACHMENT "A-2"**PREMISES TO BE SEARCHED – SUBJECT PREMISES 2**

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

304 East Silverado Ranch Boulevard, Building 8, Apartment 1110, Las Vegas, Nevada 89183 is an apartment leased by Patricia ENGSTROM. Subject Premises is a two story, multi-family apartment building having a primarily tan stucco exterior with brown trim. The apartment has a single car garage door, on the north side of the building that is tan in color and faces north. The numbers "1110" are black in color on a white placard and is affixed to the right side of the front door. The front door of the residence is tan in color and faces the south. Photo of Residence:



ATTACHMENT "B"**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
4 control the device, such as viruses, Trojan horses, and other forms of
5 malicious software, as well as evidence of the presence or absence of security
6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
14 well as documentation and manuals, that may be necessary to access the
15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
17 device;
- 18 ix. records of or information about the device's Internet activity, including
19 firewall logs, caches, browser history and cookies, "bookmarked" or
20 "favorite" web pages, search terms that the user entered into any Internet
21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;

9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.

13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED.

DATED: 3:09 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
6145 HARRISON DRIVE, SUITE 4,
LAS VEGAS, NEVADA 89120

Case No. 2:21-mj-516-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-3.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Daniel J. Albregts
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: June 17, 2021 2:34 p.m.City and state: Las Vegas, Nevada

Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
Printed name and title

Return

Case No.:
2:21-mj-516-DJA

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title



SEALED

ATTACHMENT "A-3"**PREMISES TO BE SEARCHED – SUBJECT PREMISES 3**

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

6145 Harrison Drive Suite #4, Las Vegas, Nevada 89120 is a warehouse space primarily utilized by Paul ENGSTROM, Vincent CUOMO and Abraham ELLIOTT. Subject Premises is a single story, warehouse and suite having a primarily brown stucco exterior. The warehouse and suite has a single car rollup door that is beige in color and faces north. The number "4" is affixed to the glass front door just above eye level. The door of the warehouse and suite is glass with black trim and faces north. The address "6145 Harrison 1-12" is affixed to the north side of the building on the far-east side and is black in color. Photo of Warehouse and Suite:



ATTACHMENT “B”**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the “Subject Offenses”), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.

3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.

5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.

7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.

9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.

15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.

21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.

23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
6 records relating to income derived from the transportation, sales, and distribution of
7 controlled substances and expenditures of money and wealth, for example, money
8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
10 automobiles, bank statements and other financial instruments, including stocks or
11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
20 foregoing categories of items to be seized:
- 21 i. evidence of who used, owned, or controlled the device at the time the things
22 described in this warrant were created, edited, or deleted, such as logs,
23 registry entries, configuration files, saved usernames and passwords,
24

documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

- ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- iii. evidence of the attachment of other devices;
- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- v. evidence of the times the device was used;
- vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;
- vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- viii. records of or information about Internet Protocol addresses used by the device;
- ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT “C”
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant (“the Search Warrant Data”) those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data (“the Search Warrant Data Copy”). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or “piggyback” warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;

9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.

13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED.

DATED: 3:09 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
10388 MIDSEASON MIST STREET,
LAS VEGAS, NEVADA 89183

Case No. 2:21-mj-517-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-4.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Daniel J. Albregts
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: June 17, 2021 2:34 p.m.

City and state: Las Vegas, Nevada



Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
Printed name and title

Inventory of the property taken and name(s) of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title



SEALED

ATTACHMENT "A-4"**PREMISES TO BE SEARCHED – SUBJECT PREMISES 4**

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

10388 Midseason Mist Street, Las Vegas, Nevada 89183 is the residential home of Abraham ELLIOTT. Subject Premises is a two story, single family residence having primarily beige stucco exterior with reddish brown trim. The residence has a single car garage door that is beige in color and faces west. The numbers "10388" are affixed to the south side of the residence above the garage. The front door of the residence is an unknown color encased by a white security door and faces west. Photo of Residence:



ATTACHMENT "B"

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
- 2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
- 4 control the device, such as viruses, Trojan horses, and other forms of
- 5 malicious software, as well as evidence of the presence or absence of security
- 6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
- 9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
- 12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
- 14 well as documentation and manuals, that may be necessary to access the
- 15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
- 17 device;
- 18 ix. records of or information about the device's Internet activity, including
- 19 firewall logs, caches, browser history and cookies, "bookmarked" or
- 20 "favorite" web pages, search terms that the user entered into any Internet
- 21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

- 4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;
- 9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.
- 13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.
- 17
18
19
20
21
22
23
24

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 3:10 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
305 ST. AUGUSTINE LANE,
HENDERSON, NEVADA 89014

Case No. 2:21-mj-518-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-5.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Daniel J. Albregts
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: June 17, 2021 2:34 p.m.

City and state: Las Vegas, Nevada



Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
Printed name and title

Return		
Case No.: 2:21-mj-518-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized: 		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____</p> <p style="text-align: right;">_____ <i>Executing officer's signature</i></p> <p style="text-align: right;">_____ <i>Printed name and title</i></p>		



SEALED

ATTACHMENT "A-5"**PREMISES TO BE SEARCHED – SUBJECT PREMISES 5**

1. The premises to be searched is described as follows, and include all locked and closed containers, including safes, lockboxes, and vehicles found on or directly adjacent to the property, found therein:

305 Saint Augustine Lane, Henderson, Nevada 89014 is a residential home leased by Virginia ENGSTROM. Subject Premises is a two story, single family residence having primarily beige stucco exterior with light brown trim. The residence has two separate garage doors that are beige in color and face east. The numbers "305" are affixed to the east side of the residence to the right side of the north garage door. The front door of the residence is brown in color and faces the east. Photo of Residence:



ATTACHMENT "B"

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
4 control the device, such as viruses, Trojan horses, and other forms of
5 malicious software, as well as evidence of the presence or absence of security
6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
14 well as documentation and manuals, that may be necessary to access the
15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
17 device;
- 18 ix. records of or information about the device's Internet activity, including
19 firewall logs, caches, browser history and cookies, "bookmarked" or
20 "favorite" web pages, search terms that the user entered into any Internet
21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

- 4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;
- 9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.
- 13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.
- 17
18
19
20
21
22
23
24

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 3:58 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 2017 CHEVROLET SILVERADO
 (VIN: 3GCUKREC0HG108984)
 NEVADA LICENSE PLATE VMD601

Case No. 2:21-mj-519-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
 (identify the person or describe the property to be searched and give its location):

Please see the Attachment A-6.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Daniel J. Albregts
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: June 17, 2021 2:34 p.m.

City and state: Las Vegas, Nevada



A handwritten signature in blue ink, appearing to read "Daniel J. Albregts".

Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
 Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 2:21-mj-519-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	<div style="text-align: center;"> _____ <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 10px;"> _____ <i>Printed name and title</i> </div>	



SEALED

ATTACHMENT "A-6"

PREMISES TO BE SEARCHED – SUBJECT VEHICLE 1

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2017 Chevrolet Pickup Truck, silver in color bearing Nevada license plate VMD601 VIN#3GCUKREC0HG108984. Current Registered Owner Vincent CUOMO, 487 Petal Dew Avenue, Las Vegas, Nevada 89183.
Photo of vehicle:



ATTACHMENT "B"**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
4 control the device, such as viruses, Trojan horses, and other forms of
5 malicious software, as well as evidence of the presence or absence of security
6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
14 well as documentation and manuals, that may be necessary to access the
15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
17 device;
- 18 ix. records of or information about the device's Internet activity, including
19 firewall logs, caches, browser history and cookies, "bookmarked" or
20 "favorite" web pages, search terms that the user entered into any Internet
21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”

17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;

9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.

13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 3:59 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 2007 BMW 328i (VIN: WBAVA33527KX79327)
 NEVADA LICENSE PLATE 12345TH

Case No. 2:21-mj-520-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
 (identify the person or describe the property to be searched and give its location):

Please see the Attachment A-7.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Daniel J. Albregts
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: June 17, 2021 2:34 p.m.

City and state: Las Vegas, Nevada



Judge's signature

 Honorable Daniel J. Albregts, U.S. Magistrate Judge
 Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return

Case No.:
2:21-mj-520-DJA

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title



SEALED

ATTACHMENT "A-7"

PREMISES TO BE SEARCHED – SUBJECT VEHICLE 2

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2007 BMW 4 door sedan, blue in color bearing Nevada license plate 12345TH VIN#WBAVA33527KX79327. Current Registered Owner Paul ENGSTROM, 487 Petal Dew Avenue, Las Vegas, Nevada 89183.
Photo of vehicle:



ATTACHMENT "B"**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
4 control the device, such as viruses, Trojan horses, and other forms of
5 malicious software, as well as evidence of the presence or absence of security
6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
14 well as documentation and manuals, that may be necessary to access the
15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
17 device;
- 18 ix. records of or information about the device's Internet activity, including
19 firewall logs, caches, browser history and cookies, "bookmarked" or
20 "favorite" web pages, search terms that the user entered into any Internet
21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;

9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.

13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 4:00 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))
 2019 NISSAN ROGUE (VIN: 5N1AT2MT9KC797793))
 NEVADA LICENSE PLATE US263P)

Case No. 2:21-mj-521-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
 (identify the person or describe the property to be searched and give its location):

Please see the Attachment A-8.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

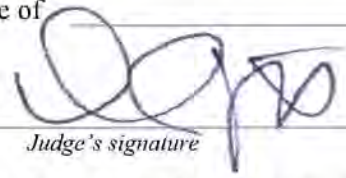
Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Daniel J. Albregts
 (United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: June 17, 2021 2:34 p.m.City and state: Las Vegas, Nevada

 Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
 Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 2:21-mj-521-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	<div style="text-align: center; margin-top: 20px;"> _____ <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 20px;"> _____ <i>Printed name and title</i> </div>	



SEALED

ATTACHMENT "A-8"

PREMISES TO BE SEARCHED – SUBJECT VEHICLE 3

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2019 Nissan SUV, silver in color bearing Nevada license plate US263P VIN#5N1AT2MT9KC797793. Current Registered Owner Paul ENGSTROM, 487 Petal Dew Avenue, Las Vegas, Nevada 89183. Photo of vehicle:



ATTACHMENT "B"**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
4 control the device, such as viruses, Trojan horses, and other forms of
5 malicious software, as well as evidence of the presence or absence of security
6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
14 well as documentation and manuals, that may be necessary to access the
15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
17 device;
- 18 ix. records of or information about the device's Internet activity, including
19 firewall logs, caches, browser history and cookies, "bookmarked" or
20 "favorite" web pages, search terms that the user entered into any Internet
21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

- 4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;
- 9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.
- 13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.
- 17
18
19
20
21
22
23
24

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 4:01 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 2016 CADILLAC CTS (VIN: 1G6AR5SS3G0195627)
 NEVADA LICENSE PLATE AL7456

Case No. 2:21-mj-522-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-9.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

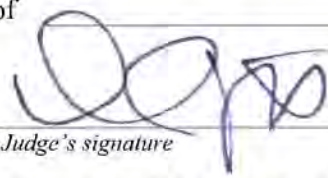
Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 *(not to exceed 14 days)*☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Daniel J. Albregts
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____Date and time issued: June 17, 2021 2:34 p.m.City and state: Las Vegas, Nevada

 Judge's signature

Honorable Daniel J. Albregts, U.S. Magistrate Judge
 Printed name and title

Return

Case No.:
2:21-mj-522-DJA

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title



SEALED

ATTACHMENT "A-9"

PREMISES TO BE SEARCHED – SUBJECT VEHICLE 4

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2016 Cadillac 4 door CTS, gray in color bearing Nevada license plate AL7456 VIN#1G6AR5SS3G0195627. Current Registered Owner Abraham ELLIOTT, 10388 Midseason Mist Street, Las Vegas, Nevada 89183. Photo of vehicle:



ATTACHMENT "B"**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- 1 documents, browsing history, user profiles, e-mail, e-mail contacts, chat and
- 2 instant messaging logs, photographs, and correspondence;
- 3 ii. evidence of the presence or absence of software that would allow others to
- 4 control the device, such as viruses, Trojan horses, and other forms of
- 5 malicious software, as well as evidence of the presence or absence of security
- 6 software designed to detect malicious software;
- 7 iii. evidence of the attachment of other devices;
- 8 iv. evidence of counter-forensic programs (and associated data) that are designed
- 9 to eliminate data from the device;
- 10 v. evidence of the times the device was used;
- 11 vi. passwords, encryption keys, biometric keys, and other access devices that
- 12 may be necessary to access the device;
- 13 vii. applications, utility programs, compilers, interpreters, or other software, as
- 14 well as documentation and manuals, that may be necessary to access the
- 15 device or to conduct a forensic examination of it;
- 16 viii. records of or information about Internet Protocol addresses used by the
- 17 device;
- 18 ix. records of or information about the device's Internet activity, including
- 19 firewall logs, caches, browser history and cookies, "bookmarked" or
- 20 "favorite" web pages, search terms that the user entered into any Internet
- 21 search engine, and records of user-typed web addresses.

22 2. As used herein, the terms "records," "documents," "programs," "applications,"
23 and "materials" include records, documents, programs, applications, and materials created,
24

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”
17
18
19
20
21
22
23
24

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;

9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.

13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.

UNITED STATES DISTRICT COURT

for the
District of Nevada

FILED

DATED: 4:01 pm, June 17, 2021

U.S. MAGISTRATE JUDGE

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 2015 CHEVROLET SONIC
 (VIN: 1G1JC6SG4F4213150)
 NEVADA LICENSE PLATE 579N08

Case No. 2:21-mj-523-DJA

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____ Nevada
(identify the person or describe the property to be searched and give its location):

Please see the Attachment A-10.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

Please see the Attachment B.

YOU ARE COMMANDED to execute this warrant on or before July 1, 2021 *(not to exceed 14 days)*☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

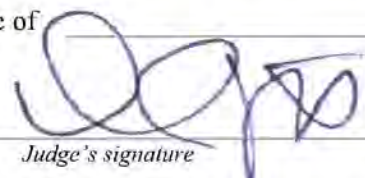
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____ Honorable Daniel J. Albregts
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____

Date and time issued: June 17, 2021 2:34 p.m.

City and state: Las Vegas, Nevada



 Judge's signature

 Honorable Daniel J. Albregts, U.S. Magistrate Judge
 Printed name and title

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means (Page 2)

Return		
Case No.: 2:21-mj-523-DJA	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	<div style="text-align: center;"> _____ <i>Executing officer's signature</i> </div> <div style="text-align: center; margin-top: 10px;"> _____ <i>Printed name and title</i> </div>	



SEALED

ATTACHMENT "A-10"

PREMISES TO BE SEARCHED – SUBJECT VEHICLE 5

1. The vehicle to be searched is described as follows, and include all locked and closed containers, including safes and lockboxes, found therein:

2015 Chevrolet 4 door hatchback, black in color bearing Nevada license plate 579N08 VIN#1G1JC6SG4F4213150. Current Registered Owner Joseph KRIEGER, 6144 Camino De Rosa Drive #3, Las Vegas, Nevada 89108. Photo of vehicle:



ATTACHMENT "B"

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 18 U.S.C. § 1956 (Money Laundering) and 21 U.S.C. §§ 841(a)(1) Distribution of and Possession with Intent to Distribute a Controlled Substance), 846 (Conspiracy to Commit Controlled Substance Offense), and 843(b) (Unlawful Use of a Communication Facility, Including the Mails, to Facilitate the Distribution of a Controlled Substance) (the "Subject Offenses"), namely:

- a. Controlled substances, including cocaine and the items commonly associated with the packaging and sales of controlled substances, including commercial plastic wrap, plastic bags or zip lock bags, film canisters, scales, or other weighing devices.
- b. Counterfeit controlled substances.
- c. Records reflecting the use of a dark web moniker or handle, or other online monikers or pseudonyms, reflecting the use of vendor or buyer accounts on dark web marketplaces.
- d. Records concerning the establishment or management of an online or dark web controlled substance retail business, including documents and other records relating to the creation or hosting of websites, evidence of dark web or Tor Browser access, merchant accounts for customer transactions, product vendors or sources of supply, invoices, order forms, and communications with co-conspirators and others about any of the aforementioned subjects.
- e. Records concerning financial transactions associated with the operations or proceeds of an online or dark web controlled substance retail business, including any paper or

- 1 digital account opening documents, statements, deposit slips, checkbooks, orders or
2 confirmations of wire transfers.
- 3 f. Records of any accounts or transactions within the traditional banking or credit
4 systems or via cryptocurrencies.
- 5 g. Digital currency, cryptocurrency (or digital currency) private keys, and digital
6 currency recovery seeds, as further explained in paragraph 4 below.
- 7 h. Packing material or inserts relating to any transactions with any cash-for-
8 cryptocurrency exchange.
- 9 i. Books, records, correspondence, narcotic customers lists, narcotic suppliers lists,
10 ledgers, logs, journals, accounts payable and receivable, pay-owe sheets, contracts,
11 letters and memoranda of agreements between potential co-conspirators, formulas,
12 receipts, phone records, phone books, address books, notations and other papers,
13 and any files relating to the transporting, ordering, purchasing, or distributing of
14 controlled substances.
- 15 j. Indicia of occupancy, residency, and/or ownership of the previously described
16 property, premises, or vehicles, and any other property, premises, or vehicles,
17 including utility and telephone bills, canceled mail, deeds, leases, rental agreements,
18 photographs, personal telephone books, diaries, envelopes, registration, receipts, and
19 keys which tend to show the identities of the occupants, residents, and/or owners,
20 not to exceed 15 items for any residence.
- 21 k. Records concerning the use of commercial mail receiving agencies and/or post office
22 boxes.
- 23 l. Photographs and/or videotapes, in particular photographs and/or videotapes of
24 potential co-conspirators and their criminal associates, assets, and/or controlled

1 substances, along with personal address lists, and other documents with the names
2 and telephone numbers of potential co-conspirators.

3 m. Records relating to the use of and accumulation of proceeds derived from the sale of
4 illegal controlled substances, as well as the acquisition of property obtained from
5 drug proceeds, and items evidencing the obtaining, secreting, transfer, concealment,
6 and/or expenditure of money obtained from drug sales, including precious metals,
7 jewelry, records of large purchases, receipts, keys and other items tending to establish
8 dominion and control of the location, canceled checks, bank records, credit card
9 records, wire transfers, wire transfer receipts, cashier's checks, cashier's check
10 receipts, addressed mail, express delivery receipts/envelopes, utility company
11 receipts, rent receipts, income tax returns, money drafts, money orders, and their
12 receipts.

13 n. Financial records including expenses incurred in obtaining the equipment and items
14 necessary for the transportation and/or distribution of controlled substances, income
15 derived from the sales of controlled substances, as well as records of legitimate
16 income or lack thereof, and general living expenses.

17 o. Financial records of persons in control of the property, premises, or vehicles,
18 including bank statements, bank receipts, passbooks, bank checks, money market or
19 similar accounts, money drafts, letters of credit, payroll documents, employer
20 information, income and expense records, Federal and State income tax returns,
21 money orders, cashier's checks, loan applications, credit card records, safe deposit
22 box and records, acquisitions, notes, and records reflecting vehicles, aircraft or
23 vessels owned, purchased, sold or leased.

- 1 p. Money counting machines, money wrappers, and/or work sheets, tally sheets, or
- 2 ledger sheets reflecting or accounting for money received, disbursed, or exchanged.
- 3 q. United States currency in excess of \$2,000, including the first \$2,000 if more than
- 4 \$2,000 is seized, digital currency such as Bitcoin stored on electronic wallets or other
- 5 forms of wallets or other means, cryptocurrency private keys and recovery seed, and
- 6 records relating to income derived from the transportation, sales, and distribution of
- 7 controlled substances and expenditures of money and wealth, for example, money
- 8 orders, wire transfers, cashier's checks and receipts, passbooks, cash cards, gift cards,
- 9 checkbooks, check registers, securities, precious metals, jewelry, antique or modern
- 10 automobiles, bank statements and other financial instruments, including stocks or
- 11 bonds in amounts indicative of the proceeds of illicit narcotic trafficking.
- 12 r. Storage units and containers, such as floor safes, wall safes, upright safes (also
- 13 known as gun safes), lock boxes, and other self-contained locked enclosures.
- 14 s. Paraphernalia for packaging, processing, cutting, weighing, and distributing
- 15 controlled substances, such as scissors, scales, funnels, sifters, grinders, glass panes
- 16 and mirrors, razor blades, plastic bags, heat-sealing devices and cutting agents.
- 17 t. Any digital device which is itself or which contains evidence, contraband, fruits, or
- 18 instrumentalities of the Subject Offenses, and forensic copies thereof.
- 19 u. With respect to any digital device containing evidence falling within the scope of the
- 20 foregoing categories of items to be seized:
 - 21 i. evidence of who used, owned, or controlled the device at the time the things
 - 22 described in this warrant were created, edited, or deleted, such as logs,
 - 23 registry entries, configuration files, saved usernames and passwords,
 - 24

- documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;
- ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- iii. evidence of the attachment of other devices;
- iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- v. evidence of the times the device was used;
- vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;
- vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- viii. records of or information about Internet Protocol addresses used by the device;
- ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

1 modified, or stored in any form, including in digital form on any digital device and any forensic
2 copies thereof.

3 3. As used herein, the term “digital device” includes any electronic system or device
4 capable of storing or processing data in digital form, including central processing units; desktop,
5 laptop, notebook, and tablet computers; personal digital assistants; wireless communication
6 devices, such as telephone paging devices, beepers, mobile telephones, and smart phones;
7 digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes);
8 peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and
9 drives intended for removable media; related communications devices, such as modems,
10 routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory
11 cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such
12 as VHS); and security devices.

13 4. Seizure of any cryptocurrency/digital currency private keys and recovery seeds
14 shall also be construed to include seizure of any cryptocurrency related to any such seized
15 private keys and/or recovery seeds, and such seizure shall allow transfer of any such related
16 cryptocurrency to one or more government controlled accounts, or “wallets.”

ATTACHMENT "C"
PROTOCOL FOR SEARCHING THE ELECTRONIC DATA SEIZED
PURSUANT TO THIS SEARCH WARRANT

1. In executing this warrant, the government must make reasonable efforts to use methods and procedures that will locate and expose in the electronic data produced in response to this search warrant ("the Search Warrant Data") those categories of data, files, documents, or other electronically stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

2. When the Search Warrant Data is received, the government will make a duplicate copy of the Search Warrant Data ("the Search Warrant Data Copy"). The original version of the Search Warrant Data will be sealed and preserved for purposes of: later judicial review or order to return or dispose of the Search Warrant Data; production to the defense in any criminal case if authorized by statute, rule, or the Constitution; for purposes of showing the chain of custody of the Search Warrant Data and the Search Warrant Data Copy; or for any other lawful purpose. The original of the Search Warrant Data will not be searched or examined except to ensure that it has been fully and completely replicated in the Search Warrant Data Copy.

3. The investigating agents will then search the entirety of the Search Warrant Data Copy using any and all methods and procedures deemed appropriate by the United States designed to identify the information listed as Information to be Seized in Attachment B. The United States may copy, extract or otherwise segregate information or data listed as Information to be Seized in Attachment B. Information or data so copied, extracted or otherwise segregated will no longer be subject to any handling restrictions that might be set out in this protocol beyond those required by binding law. To the extent evidence of crimes not within the scope of this warrant appear in plain view during this review, a supplemental or "piggyback" warrant will be applied for in order to further search that document, data, or other item.

4. Once the Search Warrant Data Copy has been thoroughly and completely examined for any document, data, or other items identified in Attachment B as Information to be Seized, and, if the

1 United States pursues a criminal prosecution in this matter, all litigation including any appeal or collateral
2 attack has been completed, the Search Warrant Data Copy will be sealed and not subject to any further
3 search or examination unless authorized by another search warrant or other appropriate Court order. The
4 Search Warrant Data Copy will be held and preserved for the same purposes identified above in Paragraph
5 2.

6 5. The search procedures utilized for this review are at the sole discretion of the investigating
7 and prosecuting authorities, and may include the following techniques (the following is a non-exclusive
8 list, as other search procedures may be used):

- 9 a. examination of all of the data contained in the Search Warrant Data to view the
10 data and determine whether that data falls within the items to be seized as set
11 forth herein;
- 12 b. searching for and attempting to recover from the Search Warrant Data any
13 deleted, hidden, or encrypted data to determine whether that data falls within
14 the list of items to be seized as set forth herein (any data that is encrypted and
15 unreadable will not be returned unless law enforcement personnel have
16 determined that the data is not (1) an instrumentality of the offenses, (2) a fruit
17 of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or
18 (5) evidence of the offenses specified above);
- 19 c. surveying various file directories and the individual files they contain;
- 20 d. opening files in order to determine their contents;
- 21 e. using hash values to narrow the scope of what may be found. Hash values are
22 under-inclusive, but are still a helpful tool;
- 23 f. scanning storage areas;
- 24 g. performing keyword searches through all electronic storage areas to determine
whether occurrences of language contained in such storage areas exist that are
likely to appear in the evidence described in Attachment A; and/or

- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

Return and Review Procedures

6. Rule 41 of the Federal Rules of Criminal Procedure provides, in relevant part:

(e) Issuing the Warrant.

(2) Contents of the Warrant.

(A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to:

(i) execute the warrant within a specified time no longer than 14 days;

(B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. . . . In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

7. Pursuant to this Rule, the government understands and will act in accordance with the following:

- a. Pursuant to Rule 41(e)(2)(A)(iii), within fourteen (14) days of the execution of the warrant, an agent is required to file an inventory return with the Court, that is, to file an itemized list of the property seized. Execution of the warrant begins when the United States serves the warrant on the named custodian; execution is complete when the custodian provides all Search Warrant Data to the United States. Within fourteen (14) days of completion of the execution of the warrant, the inventory will be filed.
- b. Pursuant to Rule 41(e)(2)(B), Rule 41(e)(2)(A) governs the time within which the electronically stored information must be seized after the issuance of the

1 warrant and copied after the execution of the warrant, not the “later review of
2 the media or information” seized, or the later off-site digital copying of that
3 media.

- 4 c. Under Rule 41(f)(1)(B), the inventory return that is to be filed with the court may
5 be limited to a description of the “physical storage media” into which the Search
6 Warrant Data that was seized was placed, not an itemization of the information
7 or data stored on the “physical storage media” into which the Search Warrant
8 Data was placed;
- 9 d. Under Rule 41(f)(1)(B), the government may retain a copy of that information
10 for purposes of the investigation. The government proposes that the original
11 storage media on which the Search Warrant Data was placed plus a full image
12 copy of the seized Search Warrant Data be retained by the government.
- 13 e. If the person from whom any Search Warrant Data was seized requests the
14 return of any information in the Search Warrant Data that is not set forth in
15 Attachment B, that information will be copied onto appropriate media and
16 returned to the person from whom the information was seized.
- 17
18
19
20
21
22
23
24